device and transmit this information to the server, the server may retrieve the security object associated with the user identification and send the security object a message requesting that the security object authenticate the security object data entered by the user. The message sent to the security object would include the security object data entered by the user which is then operated on by the methods of the security object.

Figure 5 is an exemplary diagram illustrating a message flow between a client device **510** and a server **520** using the security object of the present invention. The message flow assumes that a security object is previously stored in a storage device **530** associated with the server **520**. The security object may be created and stored in the storage device **530** in any appropriate manner. For example, a graphical user interface (GUI) may be provided through which the user may provide the security object data and optionally one or more attributes. The GUI may be provided by the client device or the server.

The GUI of the present invention acts as a "security object foundry" where a user may generate security objects of one or more types. For example, the user of the security object foundry may be provided with one or more themes including audio security objects, visual security objects, GPS location based security objects, alphanumeric security objects, biometric data based security objects, and the like. The user may select a theme and be provided with prompts for providing security object data and for selecting the methods and attributes to be encapsulated with the security object data.